When a problem asks you to show that some statement is true, this means that you should give a logical mathematical argument why the statement is always true.

1. (a) Make a list of the 16 primitive Pythagorean triples (a, b, c) with $c \leq 100$, regarding (a, b, c) and (b, a, c) as the same triple.

Solution: Plugging in values for p and q of opposite parity in the formulas $x = 2pq$, $y = p^2 - q^2$, $z = p^2 + q^2$ gives the triples $(4, 3, 5)$, $(12, 5, 13)$, $(8, 15, 17)$, $(24, 7, 25)$, $(20, 21, 29)$, $(40, 9, 41)$, $(12, 35, 37)$, $(60, 9, 61)$, $(28, 45, 53)$, $(56, 33, 65)$, $(84, 13, 85)$, $(16, 63, 65)$, $(48, 55, 73)$, $(80, 39, 89)$, $(36, 77, 85)$, $(72, 65, 97)$.

(b) How many more would there be if we allowed nonprimitive triples?

Solution: For the primitive triple $(4, 3, 5)$ we get 19 nonprimitive triples with $c \leq 100$ by multiplying $(4, 3, 5)$ by $2, 3, 4, \cdots, 20$. Similarly, $(12, 5, 13)$ gives 6 more, $(8, 15, 17)$ gives 4 more, $(24, 7, 25)$ gives 3 more, $(20, 21, 29)$ gives 2 more, and both $(40, 9, 41)$ and $((12, 35, 37)$ give 1 more, for a grand total of 36 more.

(c) How many triples (primitive or not) are there with $c = 65$?

Solution: The two in part (a) are $(56, 33, 65)$ and $(16, 63, 65)$. There are two more that are not primitive, obtained by multiplying $(4, 3, 5)$ by 13 and $(12, 5, 13)$ by 5, so the total number is 4.

2. (a) Find all the positive integer solutions of $x^2 - y^2 = 512$ by factoring $x^2 - y^2$ as $(x + y)(x - y)$ and considering the possible factorizations of 512.

Solution: The equation $(x + y)(x - y) = n$ can be solved by factoring n as $n = pq$ to obtain two equations $x + y = p$ and $x - y = q$. Solving for x and y, we get $x = (p+q)/2$ and $y = (p-q)/2$. In order for x and y to be positive integers, p and q must have the same parity (both even or both odd), and we must have $p > q$. For $n = 512 = 2^9$ the only possibilities are then $(p, q) = (256, 2)$, $(128, 4)$, $(64, 8)$, $(32, 16)$ with corresponding solutions $(x, y) = (129, 127)$, $(66, 62)$, $(36, 28)$, $(24, 8)$.

(b) Show that the equation $x^2 - y^2 = n$ has only a finite number of integer solutions for each value of n.

Solution: There are only a finite number of factorizations $n = pq$, and by part (a) each such factorization gives at most one solution $(x, y) = \big((p + q)/2, (p - q)/2\big)$, so this means there are only finitely many solutions in total, for a fixed value of n.

(c) Find a value of n for which the equation $x^2 - y^2 = n$ has at least 100 different positive integer solutions.

Solution: Generalizing part (a), if we take $n = 2^{201}$ we get 100 different factorizations $n = pq$ with $(p,q) = (2^{200}, 2), (2^{199}, 2^2), \cdots, (2^{101}, 2^{100})$ and each of these factorizations gives a different solution (x,y) (because the numbers $p = x+y$ and $q = x-y$ are uniquely determined by x and y).

Another possibility would be to build n from distinct prime factors. For example, if n is a product of 8 distinct odd primes, say $n = 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23$, then this yields 2^8 factorizations $n = pq$, but if we allow interchanging p and q to get $p > q$ this number drops to $2^7 = 128$. Note that the number n in this case is much smaller than 2^{201}.

3. Show that there are only a finite number of Pythagorean triples (a,b,c) with a, b, or c equal to a given number n.

Solution: Since a and b are interchangeable, we only need to show this for a and c. For the case of c, if c is a given number n then from $a^2+b^2 = n^2$ we get that $a^2 \le n^2$ and $b^2 \le n^2$, so $a \le n$ and $b \le n$. This limits a and b to finitely many possibilities.

If a is a given number n then the equation can be rewritten $c^2 - b^2 = n^2$. Part (b) of the previous problem then gives the desired result.

4. Find an infinite sequence of primitive Pythagorean triples where two of the numbers in each triple differ by 2.

Solution: Since we are looking for primitive triples we can use the formulas $a = 2pq$, $b = p^2 - q^2$, $c = p^2 + q^2$. If we try to make a and b differ by 2 we get the equation $2pq - p^2 + q^2 = \pm 2$, and as the left side of the equation doesn't factor, it's not clear how to find solutions. If we try to make a and c differ by 2 we get the equation $p^2+q^2-2pq = 2$, or $(p-q)^2 = 2$. Since 2 is not a square, there are no integer solutions here. The last possibility is that b and c differ by 2, so $(p^2+q^2) - (p^2-q^2) = 2$, which is equivalent to $2q^2 = 2$ or $q^2 = 1$. Taking $q = 1$ and p to be any even integer $2k$ (so that p and q have opposite parity) we get $a = 4k$, $b = 4k^2 - 1$, $c = 4k^2 + 1$ for $k = 1, 2, \cdots$.

5. Find a right triangle whose sides have integer lengths and whose acute angles are close to 30 and 60 degrees by first finding the irrational value of r that corresponds to a right triangle with acute angles exactly 30 and 60 degrees, then choosing a rational number close to this irrational value of r.

Solution: The point on the unit circle making a 60 degree angle with the x-axis is

$(x, y) = (1/2, \sqrt{3}/2)$. This gives

$$r = \frac{x}{(1-y)} = \frac{1/2}{1-\sqrt{3}/2} = \frac{1}{2-\sqrt{3}} = 2+\sqrt{3}$$

which is approximately 3.732. This is approximately $3.75 = 15/4$ so we take $(p,q) = (15,4)$. This yields the Pythagorean triple $(a,b,c) = (2pq, p^2-q^2, p^2+q^2) = (120, 209, 241)$. This has c approximately equal to $2a$, as it would be in a 60 degree right triangle.

6. Find a right triangle whose sides have integer lengths and where one of the nonhypotenuse sides is approximately twice as long as the other, using a method like the one in the preceding problem. (One possible answer might be the $(8,15,17)$ triangle, or a triangle similar to this, but you should do better than this.)

Solution: This time we take $(x,y) = (2/\sqrt{5}, 1/\sqrt{5})$ for the exact triangle. This gives

$$r = \frac{x}{(1-y)} = \frac{2/\sqrt{5}}{1-1/\sqrt{5}} = \frac{2}{\sqrt{5}-1} = \frac{\sqrt{5}+1}{2}$$

which is approximately 1.618. Approximating this by $1.625 = 13/8$ means we take $(p,q) = (13,8)$ so $(a,b,c) = (208, 105, 233)$, with 208 being approximately twice 105.

7. Find a rational point on the sphere $x^2+y^2+z^2 = 1$ whose x, y, and z coordinates are nearly equal.

Solution: When the coordinates are exactly equal we have $x = y = z = 1/\sqrt{3}$. Substituting into the formulas $u = x/(1-z)$ and $v = y/(1-z)$ leads to the values $u = v = (\sqrt{3}+1)/2$. If we approximate $\sqrt{3} = 1.732\ldots$ by $\frac{5}{3}$, this gives $u = v = (\frac{5}{3}+1)/2 = \frac{4}{3}$. The correspond point on the sphere is

$$(x,y,z) = \Big(\frac{2u}{u^2+v^2+1}, \frac{2v}{u^2+v^2+1}, \frac{u^2+v^2-1}{u^2+v^2+1}\Big) = \Big(\frac{24}{41}, \frac{24}{41}, \frac{23}{41}\Big)$$

Other answers are possible by choosing an approximation to $\sqrt{3}$ different from $\frac{5}{3}$. For example, using $\frac{7}{4}$ gives the point $\left(\frac{88}{153}, \frac{88}{153}, \frac{89}{153}\right)$.

8. (a) Derive formulas that give all the rational points on the circle $x^2+y^2 = 2$ in terms of a rational parameter m, the slope of the line through the point $(1,1)$ on the circle.

Solution: The line has equation $y-1 = m(x-1)$. Solving for y gives $y = m(x-1)+1$ and plugging this into $x^2+y^2 = 2$ yields $x^2+[m(x-1)+1]^2 = 2$. After expanding this and simplifying we get the quadratic equation

$$(1+m^2)x^2 + (2m-2m^2)x + (m^2-2m-1) = 0$$

Then the quadratic formula gives

$$x = \frac{2(m^2-m) \pm \sqrt{4(m^2-m)^2 - 4(1+m^2)(m^2-2m-1)}}{2(1+m^2)}$$

After simplification this becomes

$$x = \frac{m^2 - m \pm (m+1)}{1+m^2}$$

The plus sign gives the value $x = 1$, which is not very interesting as this leads to the original point $(1,1)$ on the circle. The minus sign gives

$$x = \frac{m^2-2m-1}{m^2+1}$$

Plugging this into the equation $y = m(x-1)+1$ then yields

$$y = \frac{-m^2-2m+1}{m^2+1}$$

(b) Using these formulas, find five different rational points on the circle in the first quadrant, and hence five solutions of $a^2+b^2 = 2c^2$ with positive integers a, b, c.

Solution: Note that we can change the signs of a, b, and c arbitrarily, and we can switch a and b. The value $m = 2$ gives $(x,y) = (-1/5, -7/5)$, or $(1/5, 7/5)$ in the first quadrant, hence a solution $(a,b,c) = (1,7,5)$. Choosing $m = 3$ happens to give the same point in the first quadrant. Choosing $m = 4$ gives $(x,y) = (7/17, -23/17)$, or $(7/17, 23/17)$ in the first quadrant, with $(a,b,c) = (7,23,17)$. We could choose other values for m to get more points, or we could just switch the x and y coordinates (hence switching a and b) to get two more points. There is also the original point $(1,1)$, corresponding to $(a,b,c) = (1,1,1)$.

(c) The equation $a^2+b^2 = 2c^2$ can be rewritten as $c^2 = (a^2+b^2)/2$, which says that c^2 is the average of a^2 and b^2, or in other words, the squares a^2, c^2, b^2 form an arithmetic progression. One can assume $a < b$ by switching a and b if necessary. Find four such arithmetic progressions of three increasing squares where in each case the three numbers have no common divisors.

Solution: In part (b) we found the solutions $(a,b,c) = (1,7,5)$ and $(7,23,17)$. These give the arithmetic progressions $1^2, 5^2, 7^2$ and $7^2, 17^2, 23^2$. Taking $m = 2/3$ gives

$(x, y) = (-17/13, -7/13)$ which yields the arithmetic progression $7^2, 13^2, 17^2$. Taking $m = 3/4$ gives $(x, y) = (-31/25, -17/25)$, which yields the arithmetic progression $17^2, 25^2, 31^2$. There are of course many other possibilities.

9. (a) For integers x, what are the possible values of x^2 modulo 8?

Solution: The eight possibilities for x modulo 8 are $0, \pm 1, \pm 2, \pm 3, 4$. Squaring these gives $0, 1, 4, 9, 16$. However, $9 \equiv 1$ and $16 \equiv 0$ mod 8, so the only squares mod 8 are $0, 1, 4$.

(b) Show that the equation $x^2 - 2y^2 = \pm 3$ has no integer solutions by considering this equation modulo 8.

Solution: If the equation had an integer solution, this would also be a solution modulo 8, so it suffices to show there are no solutions mod 8. By part (a) there are 3 choices $0, 1, 4$ for each of x^2 and y^2 mod 8. This gives 9 possibilities for $x^2 - 2y^2$, namely $0 - 2(0) = 0$, $1 - 2(0) = 1$, $4 - 2(0) = 4$, $0 - 2(1) = -2$, $1 - 2(1) = -1$, $4 - 2(1) = 2$, $0 - 2(4) \equiv 0$, $1 - 2(4) \equiv 1$, and $4 - 2(4) \equiv 4$. In summary, the possible values of $x^2 - 2y^2$ mod 8 are $0, \pm 1, \pm 2, 4$ mod 8. In particular we never get ± 3 mod 8. Thus the equation $x^2 - 2y^2 = \pm 3$ has no solutions mod 8 so it has no actual integer solutions.

(c) Show that there are no primitive Pythagorean triples (a, b, c) with a and b differing by 3.

Solution: Since we are dealing with primitive Pythagorean triples we have $a = 2pq$ and $b = p^2 - q^2$, so we are asking whether the difference $b - a = p^2 - q^2 - 2pq$ can equal ± 3. There is a little trick to simplify $p^2 - q^2 - 2pq$ by writing it as $(p - q)^2 - 2q^2$, which has the form $x^2 - 2y^2$ for $x = p - q$, $y = q$. Thus if the equation $p^2 - q^2 - 2pq = \pm 3$ had an integer solution, so would the equation $x^2 - 2y^2 = \pm 3$. But we showed in part (b) that this doesn't happen.

10. Show that for every Pythagorean triple (a, b, c) the product abc must be divisible by 60. (It suffices to show that abc is divisible by 3, 4, and 5.)

Solution: The first thing to notice is that if this is true for primitive triples (a, b, c) then it is true for nonprimitive triples as well since these are obtained by multiplying each of a, b, c in a primitive triple by some integer n. So we can assume that (a, b, c) is a primitive Pythagorean triple. Then $abc = (2pq)(p^2 - q^2)(p^2 + q^2)$, which can be rewritten as $2pq(p^4 - q^4)$ if we want. This is divisible by 4 since the first factor $2pq$ will be divisible by 4 unless p and q are both odd, but in this case the factor $2pq$ is divisible by 2 and the factor $p^2 + q^2$ is also divisible by 2 (since p^2 and q^2 are both odd) so the product abc is divisible by 4.

Next let's check that abc is divisible by 3 by seeing that its value must be 0 modulo 3. The possibilities for p and q modulo 3 are 0 and ± 1. If either p or q is 0 mod 3 then the factor $2pq$ is 0 mod 3 hence abc is 0 mod 3. The only other possibility is that p and q are both ± 1 mod 3. Then p^2 and q^2 are both 1 mod 3 so the factor $p^2 - q^2$ of abc is 0 mod 3. Hence in all cases abc is 0 mod 3.

Checking that 5 divides abc is similar. Mod 5 the possible numbers are $0, \pm 1, \pm 2$. If either p or q is 0 mod 5 then the factor $2pq$ is 0 mod 5 and abc is divisible by 5. If neither p nor q is 0 mod 5, then they are ± 1 or ± 2, so p^4 and q^4 are $(\pm 1)^4 = 1$ or $(\pm 2)^4 = 16 \equiv 1$. Then $p^4 - q^4 \equiv 0$ so 5 divides $p^4 - q^4$ hence 5 divides $abc = 2pq(p^4 - q^4)$.

This finishes the proof. Notice incidentally that for the Pythagorean triple $(3, 4, 5)$ we have $abc = 60$ so there can be no number larger than 60 that divides abc for all Pythagorean triples.